


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
**Search:** ☒ The ACM Digital Library ☐ The Guide


Searching within **The ACM Digital Library** with **Advanced Search**: ("electronic voting") and (signature) ([new search](#))

Found **13** of **257,584**

## REFINE YOUR SEARCH

### ▼ Refine by Keywords


Discovered Terms

### ▼ Refine by People

[Names](#)  
[Institutions](#)  
[Authors](#)  
[Reviewers](#)

### ▼ Refine by Publications

[Publication Year](#)  
[Publication Names](#)  
[ACM Publications](#)  
[All Publications](#)  
[Content Formats](#)  
[Publishers](#)

### ▼ Refine by Conferences

[Sponsors](#)  
[Events](#)  
[Proceeding Series](#)

[Search Results](#)
[Related Journals](#)
[Related Magazines](#)
[Related SI](#)
[Related Conferences](#)

Results 1 - 13 of 13

Sort by  in

[Save results to a Binder](#)

#### 1 [Practical multi-candidate election system](#)

[Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Gu](#)  
 August 2001 **PODC '01**: Proceedings of the twentieth annual ACM symposium on distributed computing

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (898.50 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 11, Downloads (12 Months): 53, Citation

The aim of electronic voting schemes is to provide a set of protocols that cast ballots while a group of authorities collect the votes and output the paper we describe a practical multi-candidate election scheme that ...

#### 2 [Paillier's cryptosystem revisited](#)

[Dario Catalano, Rosario Gennaro, Nick Howgrave-Graham, Phong Q. Nguyen](#)  
 November 2001 **CCS '01**: Proceedings of the 8th ACM conference on Computer Communications Security

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (1.55 MB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 4, Downloads (12 Months): 90, Citation

We re-examine Paillier's cryptosystem, and show that by choosing a particular log base  $g$ , and by introducing an alternative decryption procedure, we can design a scheme to allow an arbitrary exponent  $e$  instead of  $N$ . The ...

#### 3 [Internet voting: will it spur or corrupt democracy?](#)

[Lance J. Hoffman](#)  
 April 2000 **CFP '00**: Proceedings of the tenth conference on Computers, freedom, privacy: challenging the assumptions

**Publisher:** ACM [Request Permissions](#)

Full text available: [Pdf](#) (66.84 KB) Additional Information: [full citation](#), [references](#), [index](#)

**Bibliometrics:** Downloads (6 Weeks): 4, Downloads (12 Months): 66, Citation

#### 4 [Unlinkable serial transactions: protocols and applications](#)

[Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag](#)  
 November 1999 **Transactions on Information and System Security (TISSEC)**

Issue 4

## ADVANCED SEARCH


[Advanced Search](#)

## FEEDBACK

[Please provide us with feedback](#)

Found **13** of **257,584**

**Publisher:** ACM  [Request Permissions](#)

Full text available:  [Pdf](#) (184.87 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#), [review](#)

**Bibliometrics:** Downloads (6 Weeks): 15, Downloads (12 Months): 81, Citation


We present a protocol for unlinkable serial transactions suitable for a variety of based subscription services. It is the first protocol to use cryptographic subscription services. The protocol prevents the service from tracking ..

**Keywords:** anonymity, blinding, cryptographic protocols, unlinkable serial

## 5 [Report of the national workshop on internet voting: issues and research](#) [C. D. Mote, Jr.](#)


May 2002 **dg.o '02**: Proceedings of the 2002 annual national conference on government research

**Publisher:** Digital Government Research Center

Full text available:  [Pdf](#) (539.99 KB) Additional Information: [full citation](#)


**Bibliometrics:** Downloads (6 Weeks): 10, Downloads (12 Months): 88, Citation

## 6 [Practical forward secure group signature schemes](#)

 [Dawn Xiaodong Song](#)

November 2001 **CCS '01**: Proceedings of the 8th ACM conference on Computer Communications Security


**Publisher:** ACM  [Request Permissions](#)

Full text available:  [Pdf](#) (291.34 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 5, Downloads (12 Months): 85, Citation


A group signature scheme allows a group member to sign messages on behalf of the group, while in case of a dispute, a designated entity can revoke a signature's originator. Group signature schemes can be used as a building block for many other cryptographic protocols.

## 7 [Preserving privacy in web services](#)

 [Abdelmounaam Rezgui, Mourad Ouzzani, Athman Bouguettaya, Brahim Medjahed](#)

November 2002 **WIDM '02**: Proceedings of the 4th international workshop on Web Information and Data Management

**Publisher:** ACM  [Request Permissions](#)


Full text available:  [Pdf](#) (238.19 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 16, Downloads (12 Months): 156, Citation

Web services are increasingly being adopted as a viable means to access applications. This has been enabled by the tremendous standardization efforts to advertise, discover, and invoke Web services. Digital government (DG)


**Keywords:** digital government, mobile agents, privacy, web services

## 8 [A verifiable secret shuffle and its application to e-voting](#)

 [C. Andrew Neff](#)

November 2001 **CCS '01**: Proceedings of the 8th ACM conference on Computer Communications Security

**Publisher:** ACM  [Request Permissions](#)


Full text available:  [Pdf](#) (216.76 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 17, Downloads (12 Months): 123, Citations

We present a mathematical construct which provides a cryptographic protocol to *shuffle* a sequence of  $k$  modular integers, and discuss its application to verifiable, multi-authority election schemes. The output ...

**Keywords:** anonymous credentials, electronic voting, honest-verifier, random permutation, universal verifiability, verifiable mix, verifiable shuffle, zero-knowledge

## 9 [Electronic voting: computerized polls may save money, protect privacy](#)

 [Lorrie Faith Cranor](#)


April 1996 **Crossroads**, Volume 2 Issue 4

**Publisher:** ACM  [Request Permissions](#)

Full text available:  [Html](#) (46.29 KB) Additional Information: [full citation](#), [references](#), [citeproc](#)

**Bibliometrics:** Downloads (6 Weeks): 4, Downloads (12 Months): 4, Citations

## 10 [Strategic directions in research in theory of computing](#)

 [Michael C. Loui](#)


December 1996 **Computing Surveys (CSUR)**, Volume 28 Issue 4

**Publisher:** ACM  [Request Permissions](#)

Full text available:  [Pdf](#) (249.34 KB) Additional Information: [full citation](#), [references](#), [citeproc](#)


**Bibliometrics:** Downloads (6 Weeks): 18, Downloads (12 Months): 107, Citations

## 11 [Law-governed interaction: a coordination and control mechanism for distributed systems](#)

 [Naitaly H. Minsky, Victoria Ungureanu](#)

July 2000 **Transactions on Software Engineering and Methodology (TOSEM)**, Issue 3

**Publisher:** ACM  [Request Permissions](#)

Full text available:  [Pdf](#) (792.05 KB) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

**Bibliometrics:** Downloads (6 Weeks): 25, Downloads (12 Months): 75, Citations

Software technology is undergoing a transition from monolithic systems according to a single overall design, into conglomerates of semiautonomous heterogeneous, and independently designed subsystems, constructed a different ...

**Keywords:** coordination of heterogeneous agents, policy enforcement, software technology


## 12 [Report of the national workshop on internet voting: issues and research](#)

[C. D. Mote, Jr.](#)

May 2000 **dg.o '00**: Proceedings of the 2000 annual national conference on digital government

government research


**Publisher:** Digital Government Research Center

Full text available:  Pdf (539.99 KB) Additional Information: [full citation](#), [abstract](#)

**Bibliometrics:** Downloads (6 Weeks): 20, Downloads (12 Months): 168, Citations

As use of the Internet in commerce, education and personal communication becomes common, the question of Internet voting in local and national elections in addition to adding convenience and precision, some believe that Internet

### 13 [Compensating for a lack of transparency](#)

 [Berry Schoenmakers](#)

April 2000 **CFP '00:** Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions

**Publisher:** ACM  [Request Permissions](#)

Full text available:  Pdf (47.18 KB) Additional Information: [full citation](#), [references](#), [index](#)

**Bibliometrics:** Downloads (6 Weeks): 1, Downloads (12 Months): 6, Citations

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2009 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)